# The ADC Password Storage

By Marcelo Calbucci

Keywords: ADC, Password, LSA, connection agreement, credential

Every time you create a new Connection Agreement with ADC, you have to give a set of credential/password for each server that ADC is going to talk to. This means you'll need a credential for the Exchange 5.5 Server and another one for the Active Directory. Then, ADC will have to store this password in a secure way in order to avoid somebody to crack into the system and stole the password.

To accomplish that task, ADC stores the password in LSA Global Secrets. The LSA is a Windows storage place usually used to store very sensitive information, like password.

The whole mechanism is very simple. When you create the new Connection Agreement, the ADC Snap-in for the MMC will do a secure RPC call to ADC and ask it to store the pair(s) of credential(s)/password(s). The RPC call goes to the ADC server that is now responsible for the connection agreement. This is because the LSA Global Secrets is stored on the individual machine, and is not replicated between member servers. It **is** replicated between DCs, but the ADC does not depend on this, so uniformly sets the password on the server that is responsible for the CA. Then ADC will identify who's impersonating the Snap-in to identify it does have the right to store these information.

ADC decides that based on the same security information that is found on the service object for the ADC service. For example, if you have your domain MyDomain, and you installed ADC on MyServer server, ADC will let you or not change the information for the credential if you have Generic Write access to the following entry on the AD:

```
CN=Active Directory Connector (MyServer),CN=Exchange
Settings,CN=MyServer,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=MyDomain
```

Once you got passed the Security check, ADC will store the pair credential/password with a timestamp into the LSA.

Only the ADC Service can read the password back. The only RPC interface that we expose is the one to set the password, but not to read it. That's why every time you are going to change a Connection Agreement, and try to change an Import or Export container or attempt to re-home a connection agreement, you're requested to enter the password again.

Since we don't store password on a per-Connection Agreement basis, if you two CAs sharing the same credential, if you change the password in one CA it will also be used by the other one. This **saves** space in the Global Secrets, and saves time when the password of a service account must be changed. An administrator only needs to update the password once per ADC server.

Now you might be asking why the timestamp information with the credential. But before we explain that, let explain when we update the timestamp.

Every time somebody sets or resets a password for a credential, the timestamp is update with the current time. Also, every time that ADC reads the password, if the timestamp is older than 7 days, we update the timestamp again with the current time. We want the timestamp to be the information of when this credential was last used.

Now, for the reason we need to know when the credential was last used.

We do that basically for two reasons. The first reason is that LSA has a very limited space. ADC can use only 64 Kbytes of space. So, if ADC allotted space on LSA start running out of space, we'll remove the oldest non-used credential. To do that we follow the following rule:

| **Total number of Credentials/Passwords** | **Expiration Limit** |
|---|---|
| **< 16** | **180 days** |
| **>= 16 and < 32** | **120 days** |
| **>= 32 and < 128** | **90 days** |
| **> 128** | **60 days** |

As you can see, any Credential/Password that hasn't been used for the last 180 days will be removed. This would be the case where you create a CA, set it to never, and after 180 you try to set its schedule to "Always" or "Scheduled". This CA won't work because the password has expired and was removed from the LSA Global Secrets.

The expiration limit can be override using the following Registry Key in days:

HKLM\System\CurrentControlSet\Services\MSADC\Parameters

"Password Expiration" – REG_DWORD

The value is the minimum number of days that a credential/password will stay in the LSA Global Secrets without expiring.

Notice that if you have a CA that is set to run on "Scheduled" or "Always" its password will never expires.